August 7, 2023
Virginia Wright
Cyber-Informed Engineering Program Manager

CRITICAL CONSEQUENCES
RETHINKING THE CYBER PROTECTION OF CRITICAL INFRASTRUCTURE

RESEARCH MENTIONED IN THIS PRESENTATION WAS DEVELOPED WITH FUNDING FROM THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA) AND THE DEPARTMENT OF ENERGY.


DISTRIBUTION STATEMENT A. DISTRIBUTION APPROVED FOR PUBLIC RELEASE, DISTRIBUTION UNLIMITED.
INL Background

- One in a network of 17 DOE national labs
- DOE’s lead lab for nuclear energy
- A major center for National Security

INL Mission
Our mission is to discover, demonstrate and secure innovative nuclear energy solutions, other clean energy options and critical infrastructure.

INL Vision
INL will change the world’s energy future and secure our critical infrastructure.

Research in the National Interest that Maintains American Competitiveness & Security
INL is engaged worldwide solving *urgent* national security challenges in critical infrastructure protection and resiliency, nuclear and radiological security, and national defense.
Unique Infrastructure and Capabilities

- Electric Grid Test Bed
- Water Security Test Bed
- Specific Manufacturing Capability
- Radiological Ranges
- Explosives Test Range
- Nuclear Materials Facilities
- Wireless Test Bed
- Cyber and Energy Security Labs

INL covers 890 square miles, nearly the size of Rhode Island.
Energy Portfolio Research Focus

- Programs aimed to increase the cybersecurity of the energy grid
  - Focused on generation, transmission and distribution
What is Cybersecurity?

(1) Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Includes prevention, damage, restoration.
Includes immediate computing hardware and information on it
CIA triad plus authentication and non-repudiation (CIANA)

Definitions drawn from: https://csrc.nist.gov/glossary/term/cybersecurity

See also: https://www.securityscientist.net/blog/the-definition-of-cybersecurity-acccording-to-nist/
What is Cybersecurity (2)

• (2) The process of protecting information by preventing, detecting, and responding to attacks.

Attack-centric
Information-centric
What is Cybersecurity (3)

• (3) Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

The things we do
CIA
Information in motion and storage
What is Cybersecurity (4)

- (4) The ability to protect or defend the use of cyberspace from cyber attacks.

Attack-centric
Where, exactly, is cyberspace?
What is Cybersecurity (5)

- (5) The prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

Includes damage, unauthorized use, and exploitation
Includes restoration
Communications-systems and information
Strengthen CIA
What is Cybersecurity (6)

• (6) Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. For example, PNT data is generated by cyber systems. Protection of the devices and systems used to generate PNT data should be considered part of cybersecurity.

# 1 with an example – Position Navigation and Timing

NIST definition of PNT: All information used to form or disseminate PNT solutions, including signals, waveforms, and network packets.

https://csrc.nist.gov/glossary/term/pnt_data
What is Operational Technology?

(1) Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

(2) The hardware, software, and firmware components of a system used to detect or cause changes in physical processes through the direct control and monitoring of physical devices.

(3) Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

(4) Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

https://csrc.nist.gov/glossary/term/operational_technology
Operational Technology vs Information Technology

LOGICAL CONTROL OVER DATA ONLY
CONCERNED WITH PROTECTION OF
DATA-AT-REST / DATA-IN-MOVEMENT

PHYSICAL CONTROL OVER ‘THINGS’;
CONCERNED WITH PROTECTION OF
OPERATIONAL PROCESS – NOT DATA

IT
CORPORATE NETWORK

OT
SITE/PLANT NETWORK

ICS
CONTROL SYSTEMS NETWORK

INFORMATION PROCESSING
CIA TRIAD
CORPORATE DATA ONLY

INFORMATION FOR PROCESS CONTROL
CIA / AIC TRIAD
PROCESS DATA

PHYSICAL PROCESSING
SRP TRIAD
PROCESS CONTROL ONLY – NO DATA

NETWORK SWITCHES
FIREWALLS
ETHERNET CONVERTERS
SDN APPLIANCES
IPv4/IPv6 APPLIANCES
6LoWi/Tu/6LoWPAN/EMBEDDED DEVICES

NOTE:

DCS
RTU
HMI
PLC

http://icsmodel.infracritical.com/
Industrial Control Systems and Safety (LOPA)

https://euceng.s5system.com/lopa/

https://www.thesafetymaster.com/risk-management/lopa-sil/
Cyber Testing for Resilient Industrial Control Systems

Test Operations

ENUMERATION
- Check-In
- Initial Testing
- Hardware Enumeration
- Software and Firmware Enumeration
- Check-Out

VULNERABILITY ANALYSIS
- Check-In
- Initial Analysis
- Hardware Testing
- Software and Firmware Analysis
- Targeted Testing
- Check-Out

Analytics and Information Sharing

ANALYTIC KNOWLEDGE BASE
- Enumeration Repository
- SBOM/HBOM
- Component Prioritization Repository
- Vulnerability Repository

ANALYSIS PRODUCTS
- Critical Components
- Common Mode Vulnerabilities
- Subcomponent Supply Chain Dependencies

Programmatic Coordination

Stakeholder Engagement
- Industry Partnerships
- Securing Energy Infrastructure Executive Task Force

Component Prioritization
Coordinated Vulnerability Disclosure

COLLABORATORS
- National Labs
- Idaho National Laboratory
- Pacific Northwest National Laboratory
- Lawrence Livermore National Laboratory
- Sandia National Laboratories
- Oak Ridge National Laboratory
- NREL
- Schneider Electric
- Hitachi Energy
- SEL

IDAHO NATIONAL LABORATORY
Objective: Enable black start recovery of the power grid amidst a cyber-attack on the energy sector's critical infrastructure.
Simulate black start recovery of a crank path amidst a cyber attack on the power infrastructure to enable grid restart operations.
RADICS Exercise Assumptions

- Live ongoing cyber attack
  - Assets and network are pwned by attacker
  - Attacker can prevent typical “Black Start” restoration
- Reflashing and restoration are not a viable solution
- Operating in manual mode is not a long-term option
- Defenders are detecting attacker tools and “reclaiming” territory
- Tool creators must work with and through power operations team
- Goal is restoration of service and control of infrastructure
Important Industry Drivers for Energy

Geopolitical

• Extreme weather / climate change
• Transition to clean energy
• Largest single federal investment in energy infrastructure
• Continued dependence on fossil fuels
• International ONG market instability
• Instability in clean energy supply chains
• Increased protectionism of US production
• Pressure on uranium production
• Nuclear industry slow to expand
• National extremism on the rise
Important Industry Drivers for Energy

Technological

• Energy diversity requires digitization, automation, integration, and orchestration
• Large changes in features and capabilities of seemingly familiar products
• Continued LONG deployments (decades)
• IT-class technology being incorporated into OT solutions
• Engineers less involved in design and operations
• Industry moving to cloud for data aggregation and in some cases, control
• Digital technology inherently vulnerable (Icefall)
• Many green energy solutions require continuous network connectivity
• Changing generation and load profiles, especially in distribution
Cyber-Informed Engineering (CIE)

- CIE uses design decisions and engineering controls to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the opportunity to use engineering to eliminate specific harmful consequences throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on engineers and technicians, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to engender a culture of security aligned with the existing industry safety culture.
National CIE Strategy

• Directed by the U.S. Congress in the Fiscal Year 2020 National Defense Authorization Act

• Outlines core CIE concepts
  − Defined by a set of design, operational, and organizational principles
  − Place cybersecurity considerations at the foundation of control systems design and engineering

• Five integrated pillars offer recommendations to incorporate CIE as a common practice for control systems engineers
  − Intended to drive action across the industrial base stakeholders—government, owners and operators, manufacturers, researchers, academia, and training and standards organizations

• DOE issued the National CIE Strategy June 15, 2022
Pillars of the National CIE Strategy

**Awareness**
Promulgate a universal and shared understanding of CIE

**Education**
Embed CIE into formal education, training, and credentialing

**Development**
Build the body of knowledge by which CIE is applied to specific implementations

**Current Infrastructure**
Apply CIE principles to existing systemically important critical infrastructure

**Future Infrastructure**
Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology
<table>
<thead>
<tr>
<th>Principle</th>
<th>Key Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence-Focused Design</td>
<td>How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?</td>
</tr>
<tr>
<td>Engineered Controls</td>
<td>How do I implement controls to reduce avenues for attack or the damage which could result?</td>
</tr>
<tr>
<td>Secure Information Architecture</td>
<td>How do I prevent undesired manipulation of important data?</td>
</tr>
<tr>
<td>Design Simplification</td>
<td>How do I determine what features of my system are not absolutely necessary?</td>
</tr>
<tr>
<td>Resilient Layered Defenses</td>
<td>How do I create the best compilation of system defenses?</td>
</tr>
<tr>
<td>Active Defense</td>
<td>How do I proactively prepare to defend my system from any threat?</td>
</tr>
<tr>
<td>Interdependency Evaluation</td>
<td>How do I understand where my system can impact others or be impacted by others?</td>
</tr>
<tr>
<td>Digital Asset Awareness</td>
<td>How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?</td>
</tr>
<tr>
<td>Cyber-Secure Supply Chain Controls</td>
<td>How do I ensure my providers deliver the security we need?</td>
</tr>
<tr>
<td>Planned Resilience</td>
<td>How do I turn “what ifs” into “even ifs”?</td>
</tr>
<tr>
<td>Engineering Information Control</td>
<td>How do I manage knowledge about my system? How do I keep it out of the wrong hands?</td>
</tr>
<tr>
<td>Cybersecurity Culture</td>
<td>How do I ensure that everyone performs their role aligned with our security goals?</td>
</tr>
</tbody>
</table>
Getting Involved

EMAIL CIE@INL.GOV
CIE COP and Working Group Purpose

**Cyber-Informed Engineering COP**
Starting Jan. 2023
Quarterly
Next Meeting – July 12, 2023, 11AM MT / 1 PM ET

- Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

**CIE Education WG**
Monthly starting Feb. 2023
3rd Wednesday, 9 AM MT / 11 AM ET

- Develop curricula and materials that integrate CIE principles into engineering degree programs

**CIE Development WG**
Monthly starting Feb. 2023
4th Wednesday, 9 AM MT / 11 AM ET

- Develop CIE implementation guidance and an open-source library of resources

**CIE Standards WG**
Monthly starting Aug. 9, 2023
1st Wednesday, 9 AM MT / 11 AM ET

- Support integration of CIE into engineering and cybersecurity standards
Upcoming CIE Presentations and Outreach

Save the Date: Cyber-Informed Engineering Practitioner’s Workshop – Multiple presentations and panels for CIE practitioners

Register for the workshop: https://mccrary.auburn.edu/events/cie-practitioners-workshop/
Recent CIE Publications

• SANS ICS Concepts Video: https://youtu.be/o_vlxW6UTeg
• CIE Workbook: https://www.osti.gov/biblio/1986517
• Industrial Cyber: CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
• Harvard Business Review: Engineering Cybersecurity into U.S. Critical Infrastructure (April 17, 2023) by Ginger Wright, Andrew Ohrt, and Andy Bochman
• Shift Left video podcast on GrammaTech blog: Shifting Left for Energy Security (April 4, 2023) with Ginger Wright, Idaho National Lab and Marc Sachs, Auburn University
• For more CIE articles and publications, visit: inl.gov/cie
Next Steps for CIE

• Expanded CIE Implementation Guidance
• Benefits quantification methodology
• Survey of applicable standards
• Multiple Curriculum Resources
  – Exercises
  – Training Guides
  – Lesson Plans
• Tool for Applying CIE at Varying Criticality Levels
• CIE Validation Methods